

A New Means and Method for Protecting  
Cryptoteleprinter TransmissionsApproved for Release by NSA on 09-10-2013  
pursuant to E.O. 13526

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
+	+		+	+		+	+		+	+		+	+		+	+		+	+		+	+		+	+		+	+		+	+
+	+			+	+			+	+			+	+			+	+			+	+			+	+			+	+		
+	+	+	+					+	+	+	+					+	+	+	+					+	+	+	+				
+	+	+	+	+	+	+	+								+	+	+	+	+	+	+	+									
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

1st level

2d "

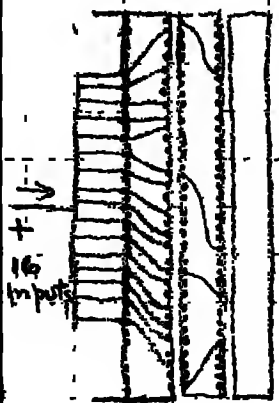
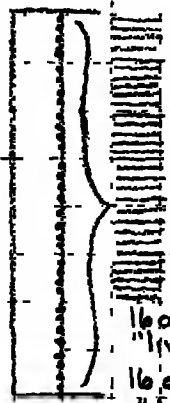
3d "

4th "

5th "

Transmitting End

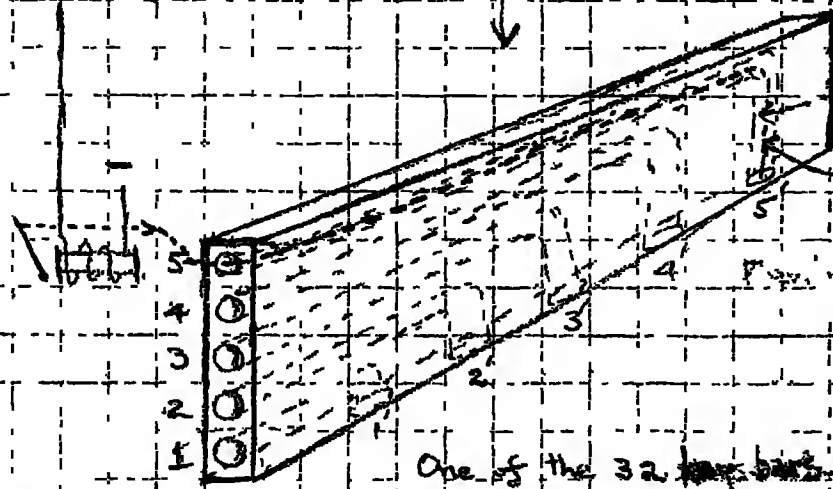
Receiving End

32 point  
rotor system  
of n rotors16 outputs  
"live"  
16 outputs  
"dead"

Go to relays or magnets controlling whether or not a "projection" presents itself under a bar

Five successive operations of the rotor system will set up the necessary permutation of + and - projections under the bars → and the end result is to set up a monoalphabet for the Baudot equivalents of the 32-character alphabet.

After each series of 5 operations of the rotor system a new monoalphabet is established.



Tube through which flexible rotor Baudot wire pushes out "projection". Magnet at left supplies motive power.

One of the 32 key bars - projection bars. The keys of keyboard actuate on depression.

These bars operate the 5 sliding bars that set up the Baudot permutation representing the letter or character to be "enciphered".

The general arrangements are the same. The rotor system must of course be an exact duplicate of, and in phase cryptographically with that at the transmitting end. Instead of controlling the "projections" under the key bars the output circuits of the rotor system control the setting up of the slots in the "translator" mechanism to correspond with the monoalphabet established at the moment by the rotor system. If the "translator" mechanism comprises the "slotted-bar" type of arrangement the analogy with the "projection bars" under the keyboard is exact.

Invented 25 Feb 1947 by  
William F. Friedman

Useful for  
Authentication  
purposes?  
Only 1-way low-  
complex but not complex

	1	2	3	4	5
1	2	3	4	5	6
2	3	4	5	6	7
3	4	5	6	7	8
4	5	6	7	8	9
5	6	7	8	9	0
6	7	8	9	0	1

2	1-1						
3	1-2	2-1					
4	1-3	2-2	3-1				
5	1-4	2-3	3-2	4-1			
6	1-5	2-4	3-3	4-2	5-1	} ← 6	} ← 8
7		2-5	3-4	4-3	5-2		
8			3-5	4-4	5-3	6-2	
9				4-5	5-4	6-3	
0					5-5	6-4	
1						6-5	

6	=	1-5	2-4	3-3	4-2	5-1
8						

II	( )
I -	( )
I r	( )
III	( )
IV	( )
V	( )
S	( )
Z	( )
X	( )
P	( )

2	2	6	1	6	6	1	8	9
---	---	---	---	---	---	---	---	---

2	2	6	1	6	6	1
---	---	---	---	---	---	---

0	1	.	6	.	6	
---	---	---	---	---	---	--

1	1	5							
---	---	---	--	--	--	--	--	--	--

3	8	2	.	1	6	.	1	9	7
---	---	---	---	---	---	---	---	---	---


0	1	6	6
---	---	---	---

2	1		5			5
---	---	--	---	--	--	---

1	6	7	1					
---	---	---	---	--	--	--	--	--

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

100